DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 28 February 2008 has been entered.

2. In response to the previous office action, Applicant has amended claims 1, 4, 9, 19, 29, and 30. Claims 1, 3-7, and 9-30 have been examined.

Allowable Subject Matter

3. Claims 1, 3-7, and 9-30 are allowed.

4. The following is an examiner's statement of reasons for allowance: The citation of different specific types of measurement values overcomes the previously cited art, Grawrock. No further art could be found that would render the claimed invention unpatentable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid, can be reached at (571) 272-4063.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Matthew Heneghan/

Primary Patent Examiner, USPTO AU 2139

April 9, 2008

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney David McKenzie on 26 March 2008.

Paragraph 37 of the specification is amended as follows:

[0037] Modules may also be implemented in software stored on a computer readable storage medium for execution by various types of processors. An identified module of executable code may, for instance, comprise one or more physical or logical blocks of computer instructions which may, for instance, be organized as an object, procedure, or function. Nevertheless, the executables of an identified module need not be physically located together, but may comprise disparate instructions stored in different locations which, when joined logically together, comprise the module and achieve the stated purpose for the module.

Claims 1, 4, 9, and 19 are amended as follows:

1. An apparatus for sealing a data repository to a trusted computing platform, the apparatus comprising:

an embedded security system (ESS) comprising at least one platform configuration register;

a measurement module configured to generate one or more measurement values for one or more devices physically connected to a computer system and to extend the measurement values to at least one platform configuration register;

a key management module configured to seal a cryptographic key associated with a data repository by cryptographically combining the cryptographic key with the measurement values for one or more of ~~a BIOS,~~ a boot record, a drive serial number, and an object code image of decryption software in at least one platform configuration register, the measurement values representing a trusted configuration of the trusted computing platform, and to unseal the cryptographic key using the measurement values by way of the ESS; and

a cryptography module configured to encrypt data stored in the data repository and to decrypt data read from the data repository with the unsealed cryptographic key.

4. A system for sealing a data repository to a trusted computing platform, the system comprising:

a data repository configured to encrypt data written to the data repository and to decrypt data read from the data repository using a cryptographic key;

an embedded security system (ESS) comprising at least one platform configuration

register;

a measuring module configured to generate one or more measurement values for one or more devices within the system and to extend the measurement values to one of the at least one platform configuration registers; and

a key management module configured to:

seal the cryptographic key associated with the data repository by cryptographically combining the cryptographic key with the at least one platform configuration register measurement value for one or more of ~~a BIOS,~~ a boot record, a drive serial number, and an object code image of decryption software, the measurement value representing a trusted configuration, and to unseal the cryptographic key using the measurement values by way of the ESS; and read a sealed cryptographic key, unseal the cryptographic key, and

provide the cryptographic key to the data repository before an operating system loads.

9. A computer readable storage medium comprising computer readable code configured to carry out a method for sealing a data repository to a trusted computing platform, the method comprising:

encrypting data on a data repository with a cryptographic key;

sealing the cryptographic key by cryptographically combining the cryptographic key with measurement values for one or more of ~~a BIOS,~~ a boot record, a drive serial number, and an object code image of decryption software, the measurement values representing a trusted configuration to a platform configuration to produce a sealed key;

unsealing the sealed key using the measurement values to produce the cryptographic key; and

decrypting data on the data repository with the unsealed cryptographic key.

19. A method for sealing a data repository to a trusted computing platform, the method comprising:

encrypting data on a data repository with a cryptographic key;

sealing the cryptographic key by cryptographically combining the cryptographic key with measurement values for one or more of ~~a BIOS,~~ a boot record, a drive serial number, and an object code image of decryption software, the measurement values representing a trusted configuration to a platform configuration to produce a sealed key;

unsealing the sealed key using the measurement values to produce the cryptographic key; and

decrypting data on the data repository with the unsealed cryptographic key.

/M. H./

Primary Examiner, Art Unit 2139